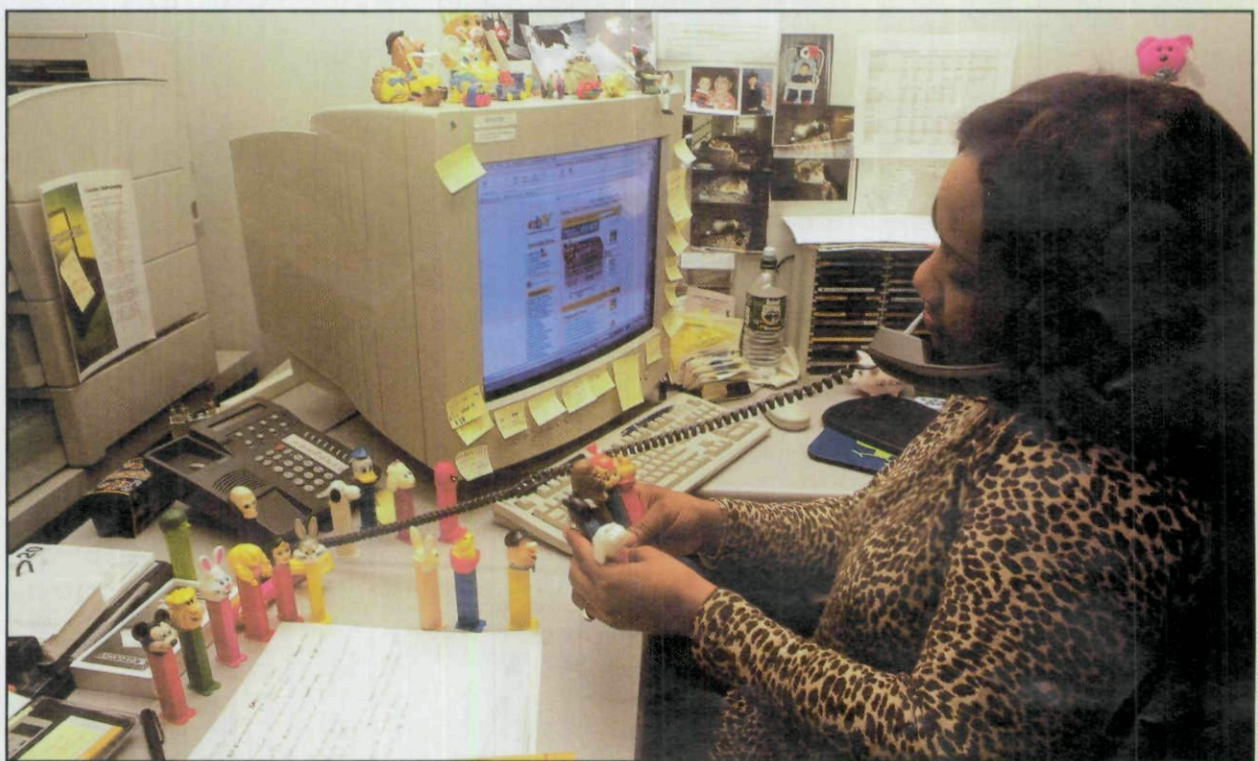


*Surveying use policies of three organizations—
educational institutions, ISPs, and non-ISPs.*

ACCEPTABLE INTERNET USE POLICY

With computers and the Internet now embedded into nearly every nook and cranny of the office environment, businesses are increasingly aware of the Internet abuse issues raised by employees using the ubiquitous technology to conduct personal online transactions or to sneak a peak at a naughty Web site. Internet abuses in the workplace include, but are not limited to,



KENG SIAU, FIONA FUI-HOON NAH, AND LIMEI TENG

accessing nonwork-related sites, email abuse, online chatting, gaming, investing, shopping, and downloading programs of personal interests, such as MP3s. They also include using the Internet too often at work, which is commonly known as cyberslacking. Ultimately, these abuses refer to employees being online at work and not doing what they're paid to do—their jobs.

This article surveys the acceptable Internet use policy (AIUP) of three groups of organizations—educational institutions, Internet service providers (ISPs), and non-ISPs. It also provides guidelines on developing an AIUP and concludes with a discussion on privacy issues in monitoring employees' Internet use.

Prime Internet Abuses

Through an extensive review of the Internet abuse literature, we identified 11 categories of Internet abuses (not mutually exclusive) and present them in Table 1.

General email abuses range from accidentally sending a personal note to everyone in the company to transmitting sexually or racially charged correspondence. The latter can create a hostile work environment for employees [1]. Some major companies have settled multimillion dollar sexual-harassment lawsuits as a result of internally circulated email. Another example of email abuse is spam. Spam refers to flooding the Internet with many copies of the same message in an attempt to force the message on people who would not otherwise choose to receive it. Spam consumes bandwidth, floods mailboxes, and slows down servers and networks.

Unauthorized Internet usage and access is another major concern, especially for ISPs [8]. The main source of revenue for ISPs comes from providing Internet access to users at a fee. Unauthorized access creates security concerns and impacts revenues. Another example is the sharing of one's password, which may jeopardize a company's trade secrets and confidential information.

One common copyright infringement violation is the posting of copyrighted material on the Web. Amendments to the Copyright Infringement Act and the Computer Fraud and Abuse Act, and enactment of the Economic Espionage Act of 1996 are some of the

Table 1. Definitions of different types of Internet abuses.

Internet Abuses	Definitions
General Email Abuses	Include spamming, harassments, chain letters, solicitations, spoofing, propagations of viruses/worms, and defamatory statements.
Unauthorized Usage and Access	Sharing of passwords and access into networks without permission.
Copyright Infringement/Plagiarism	Using illegal or pirated software that cost organizations millions of dollars because of copyright infringements. Copying of Web sites and copyrighted logos.
Newsgroup Postings	Posting of messages on various nonwork-related topics from sex to lawn care advice.
Transmission of Confidential Data	Using the Internet to display or transmit trade secrets.
Pornography	Accessing sexually explicit sites from work place as well as the display, distribution, and surfing of these offensive sites.
Hacking	Hacking of Web sites, ranging from denial-of-service attacks to accessing organizational databases.
Nonwork-Related Download/Upload	Propagation of software that ties up office bandwidth. Programs such as Gnutella and Napster allow the transmission of movies, music, and graphical materials.
Leisure Use of the Internet	Loafing around the Internet, which includes shopping, sending e-cards and personal email, gambling online, chatting, game playing, auctioning, stock trading, and doing other personal activities.
Usage of External ISPs	Using an external ISP to connect to the Internet to avoid detection.
Moonlighting	Using office resources such as networks and computers to organize and conduct personal business (side jobs).

laws that protect intellectual property rights.

Newsgroup postings not only take up bandwidth but also waste precious office hours and resources as workers scour discussion groups to express opinions. They can also be a nuisance if one chooses to post his or her views on many discussion boards, similar to the case of spamming.

The transmission of confidential data and trade secrets by employees is a violation of nondisclosure agreements set forth by their companies. Any intellectual work and product used for a business purpose or software that contains novel or unique elements, procedures, or compilations can be classified as a trade secret.

It is estimated one in five white-collar male workers access pornography at work [1]. However, pornography alone is not the only cause of Internet misuse. Surfers are also accessing news, information, and finance sites to keep up with the latest news or stock quotes.

Hacking involves the act of exploiting weaknesses in Web site security to access proprietary data such as confidential information or passwords [2]. Some users hack just for the fun of it, to prove they can, while others may hack just to gather enough information to use

Table 2. Internet abuses addressed by AIUPs of ISPs.

Internet abuses	Internet Service Providers													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
General Email Abuses	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Unauthorized Usage and Access			X		X	X	X	X	X	X	X	X	X	X
Copyright Infringement/Plagiarism		X		X					X	X		X	X	X
Newsgroup Postings	X		X	X	X	X	X	X	X	X		X	X	X
Transmission of Confidential Data											X	X	X	X
Pornography					X		X							
Hacking		X				X			X	X			X	X
Nonwork-Related Download/Upload			X	X				X						
Leisure Use of the Internet						X								
Usage of External ISPs					X									
Moonlighting														

Table 3. Internet abuses addressed by AIUPs of Educational institutions.

Internet Abuses	Educational Institutions													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
General Email Abuses	X		X	X	X	X	X		X	X	X	X	X	X
Unauthorized Usage and Access	X		X	X	X	X	X		X	X	X	X	X	X
Copyright Infringement/Plagiarism	X	X	X	X	X			X	X	X	X	X	X	X
Newsgroup Postings	X				X						X		X	X
Transmission of Confidential Data	X				X							X		X
Pornography					X							X	X	X
Hacking	X								X	X				
Nonwork-Related Download/Upload	X		X							X		X		X
Leisure Use of the Internet									X					
Usage of External ISPs				X										
Moonlighting														

respondents acknowledged having accessed nonwork-related sites approximately an hour each week, while 30% admitted to watching sports online during work at least once a month. Approximately 27% revealed they accessed stock trading sites at work. Game playing on office computers actually costs businesses about \$50 billion a year [10], and middle managers are the biggest perpetrators.

Using external ISPs to access the Internet at work to avoid detection is another form of Internet abuse. Despite the use of external ISPs, employees are still misusing the company's communication lines and resources.

Moonlighting is an increasing problem. As a company's technological resources advance and network connections pump up, employees may utilize these resources to work on an external assignment for additional income. These culprits include programmers, system analysts, and those equipped with advanced skills like Java, C++, and XML. Moonlighting is becoming a "great adventure" not only because of the shortage of talent in the market, but also because of the allure of an entrepreneurial life that can share equity in start-up technology projects. The thrill of getting involved in the next Yahoo! is difficult to resist.

Nearly two-thirds of U.S. firms have disciplined employees for Internet abuses [4]. Among those

certain online services for free.

Nonwork-related downloading and uploading of materials is another issue. Napster, the controversial former site that permitted users to download and upload songs took up over 80% of the bandwidth at some workplaces [1]. Napster is the type of technological innovation that created overworked bandwidths, introduced new legal hassles, and hindered productivity in the office.

Loafing around the Internet covers personal activities such as paying personal bills, playing games, stock trading, auctioning of personal items, gambling, and chatting. In a recent survey by Websense [9], 57% of 300

that combat against inappropriate usage, 45% utilized AIUP [5]. *Internet Week* also reported that 45% of IT managers surveyed said they have established AIUP to combat Internet abuses [11].

Acceptable Internet Use Policy

This section presents a content analysis of the AIUPs of three groups of organizations—educational institutions, ISPs, and non-ISPs. The non-ISPs include private organizations, government offices, nonprofit organizations, and public libraries. The AIUPs of ISPs are catered to their subscribers and members, whereas the AIUPs of non-ISPs and educational institutions are

designed with employees and users of their networks in mind. This survey includes organizations from different parts of U.S. Tables 2, 3 and 4 summarize the results of the content analysis.

Comparing AIUPs of the Three Groups

Every ISP and non-ISP surveyed addressed email abuses in their AIUPs (see Tables 2 and 4). Referring to Table 3, 12 out of 14 educational institutions surveyed included email abuses in their AIUPs. The more specific email abuses mentioned in the AIUPs of these educational institutions are sexual harassment, spamming, and solicitation ranging from personal sales to political lobbying.

Most organizations in the three groups also have policies against copyright infringements and plagiarism. These days, it is important to have policies that clearly define copyright and licensing of programs and software because copyright lawsuits could cost millions.

We also observe some differences between the three groups. As shown in Table 2, ISPs are particularly apprehensive about newsgroup postings. Flaming, sexual harassment, and hate-messages in

Another difference between the three groups is ISPs and educational institutions address unauthorized usage and access in their AIUPs to a greater degree than non-ISPs.

ISPs and educational institutions do not place as much emphasis against leisure surfing as non-ISPs. This is not surprising because ISPs provide Internet access to the public at a fee and educational institutions encourage the self-exploration of information online to aid in the teaching and research profession. On the other hand, it is important for non-ISPs to discourage their employees from surfing nonwork-related sites.

Some AIUPs address individual company needs. In the case of a non-ISP (company #8 in Table 4), a policy specifically targeting problems in leisure surfing is in place. According to its policy, employees can have access to the Internet for less than 30 minutes a day. Any extra usage must be approved by a supervisor prior to using the system.

Guidelines to Develop AIUP

The role of AIUP is to provide a general usage guideline, not to control users [6]. On one hand, AIUP

should be as comprehensive as possible. On the other hand, AIUP should not be so restrictive that it gets in the way of productive exploration or suffocates employees. Finding a balancing point is the key. The following are some guidelines:

- State the company's values. These values may include profit-making, professionalism, and cost-saving endeavors.
- The AIUP should complement the Code for Ethical Computer Use, and other codes and poli-

cies of the company.

- Make it clear the company's system should be used only for business purposes.
- Emphasize that the company reserves the right to monitor all forms of Internet and email use, and list all types of monitoring carried out.
- Stress that transmission, display, or storage of sexually explicit, defamatory, or offensive materials is strictly prohibited at all times.
- Enforce policy in a consistent and uniform manner, and assure disciplinary action will follow if there is a violation of policy.
- Involve employees in the AIUP development process and ensure that employees understand and agree with the policy.

Table 4. Internet abuses addressed by AIUPs of non-ISPs.

Internet Abuses	Non-ISPs									
	1	2	3	4	5	6	7	8	9	10
General Email Abuses	X	X	X	X	X	X	X	X	X	X
Unauthorized Usage and Access			X			X	X		X	X
Copyright Infringement/Plagiarism	X			X	X		X		X	X
Newsgroup Postings						X			X	
Transmission of Confidential Data					X		X		X	
Pornography		X	X				X	X	X	
Hacking						X				X
Nonwork-Related Download/Upload										
Leisure Use of the Internet		X					X	X	X	
Usage of External ISPs						X				
Moonlighting									X	

newsgroup postings can create serious problems. Excessive messaging can also flood networks, which in turn can cause servers to shut down. Most non-ISPs and educational institutions, however, do not have any statement in their policies regarding newsgroup postings.

Among the three groups, ISPs seem to be most concerned about hacking. One explanation is these ISPs generate revenue by providing services. Unauthorized access to customer information ranging from email addresses to credit card numbers could seriously harm their image. Although non-ISPs and educational institutions are concerned about hacking as well, they do not seem to address that concern in their policies.

Monitoring Software—A Solution or a Privacy Issue

Monitoring software is increasingly used to combat Internet abuses. According to International Data Corporation (IDC), about 40% of companies use monitoring software, an increase of 23% compared to the number in late 1998. IDC predicted that by July 2001, 80% of companies would be monitoring their employees' online behavior [4]. Statistics have shown 58% of employers who monitor Internet usage do so to control recreational use; 47% do so to reduce bandwidth abuse; 47% do so to eliminate downloads of pirated software; and 33% monitor to reduce sluggish Internet connections due to nonwork-related use [3].

Employees' email is a prime target for monitoring. Workplace email accounts should be perceived as an "unsecured filing cabinet" used for official business only, and employers have unbridled right to access such accounts at any time they want. Email is scrutinized to safeguard intellectual assets, to detect nonwork-related usage, to defend against viruses, and to prevent sexual and racial harassment lawsuits. A recent survey by the American Management Association found the percentage of major U.S. companies monitoring employee email has increased from 15% in 1997 to nearly 40% in early 2000 [7].

Monitoring where employees surf is also common. Many employees and privacy groups say it is all right to monitor excessive usage but disagree when it comes to monitoring where employees surf, as the latter gives insights to the most personal and private aspects of their lives. For example, employees would not like their employers to have knowledge they had recently sought online advice for family violence or ordered AZT (an antiviral drug used for the treatment of AIDS) from an online pharmacy. Also, employees may worry their employers are collecting evidence against them that may later turn up in their human resource files.

In order to create a harmonious working atmosphere, there must be a certain degree of control bonded together with adequate sensitivity training for both employees and employers. In this fast-paced society, employees are literally working overtime just to satisfy company needs. So where do they find the time to complete little errands? The company needs to realize certain personal business, like making sure the wife gets her dozen roses on time for an anniversary and the bank takes care of the mortgage on time, may need to be conducted during work hours. According to a survey by Websense [9], 68% of the respondents indicated they should be allowed to access nonwork-related Web sites at break times, as well as before and after work. About half of the 300 respondents said that one half of an hour per day is the appropriate time to allocate to each employee.

Conclusion

Internet access needs to be managed properly and professionally. Management should inform employees in what ways they are being monitored. When there is a new policy or changes to an existing policy, employees should be notified.

We found that most AIUPs are not formally worded or legally sound. Legal assistance should be obtained in developing AIUPs. The AIUPs we have reviewed do not include a comprehensive coverage of Internet abuses, as shown in Tables 2, 3, and 4. All Internet abuses should be addressed in AIUPs in order to eliminate "gray areas" and prevent anyone from "escaping" just because it is not written in black and white.

Companies should always back up policies with decisive actions. They should be immaculately consistent and follow whatever disciplinary actions indicated in the policy. This means employees who have violated the policy should be disciplined, and the employer has to be consistently fair in carrying out such actions. Establishing a chain of command between the IT department and other departments is also encouraged. This is a good way of allowing the culprit's department head to be responsible for disciplining him or her instead of overloading the IT department with such issues. **G**

REFERENCES

1. Conlin, M. Workers, surf at your own risk. *Business Week Online*. (Aug. 4 1997); www.businessweek.com/2000/00_24/b3685257.htm.
2. Csinger, A. and Siau, K. The global public key infrastructure: Terms and concepts. *IEEE Comput.* 31, 9 (Sept. 1998), 30–31.
3. Center for On-Line Addiction. Dealing with Internet misuse in the workplace; www.netaddiction.com/workplace.htm.
4. Greengard, S. The high cost of cyberslacking. *Workforce Online*. (Dec. 2000); www.workforce.com/archive/article/000/58/01.xci.
5. InternetWeek Online. Internet usage policies (Oct. 15, 1999); www.internetwk.com/numbers/numbers101599.htm.
6. Kallman, E.A. and Grillo, J.P. *Ethical Decision Making and Information Technology: An Introduction with Cases*. McGraw-Hill, New York, 1996.
7. Schwartz, K.D. We've got mail. *CIO Magazine* (Sept. 15, 2000); www2.cio.com/archive/091500_mail_content.html.
8. Siau, K., Lim, E., and Shen, Z. Mobile commerce—Promises, challenges, and research agenda. *J. Database Manag.* 12, 3 (Jul.-Sept. 2001), 4–13.
9. Websense Inc. Online. Web@Work study. (Feb. 2001); www.websense.com/.
10. DVD Software, Inc. Workers abuse computer games. *Futurist* 31, 3 (May/June 1997), 13.
11. Yasin, R. Web slackers put on notice. *Internet Week Online Archives* (Oct. 15, 1999); www.internetwk.com/lead/lead101599.htm.

KENG SIAU (ksiau@unl.edu) is an associate professor of MIS at the University of Nebraska-Lincoln and the editor-in-chief of *Journal of Database Management*.

FIONA NAH (fnah@unl.edu) is an assistant professor of MIS at the University of Nebraska-Lincoln.

LIMEI TENG is an IT professional in Singapore.

Copyright of Communications of the ACM is the property of Association for Computing Machinery. The copyright in an individual article may be maintained by the author in certain cases. Content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.